Be Alert!

This counterintelligence awareness booklet is provided courtesy of the Office of the National Counterintelligence Executive (ONCIX)

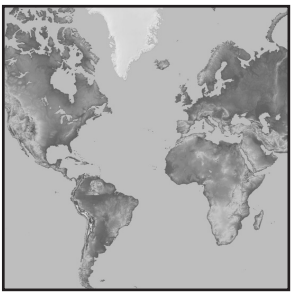
ONCIX Mailing Address:
Crystal Square 5, Room 301
Washington, DC 20505
Web site: http://www.ncix.gov/

Table of Contents

Prepared by
The Office of the National Counterintelligence Executive
www.ncix.gov

You Are the Target

In a world that increasingly measures national power and security in economic as well as military terms, US citizens traveling abroad continue to be the target of foreign intelligence collection activities. Many foreign governments and foreign businesses place a high priority on acquiring US Government and private industry– protected information (classified, sensitive, and proprietary). Although the Cold War has ended, the risk of becoming an intelligence target has increased. The threat you face as an official US Government traveler or as a representative of private industry is real. This pamphlet describes the nature of the foreign intelligence collection threat, provides basic steps you can take to mitigate the threat, and actions you should take to report suspicious incidents.



Each year, the number of suspicious incidents involving the targeting of US-protected information and trade secrets reported to federal authorities has increased. Newspaper reports about recent espionage arrests only serve to underscore our continued national concerns. Although news articles may focus on one or two countries, US official and private industry travelers have reported incidents occurring throughout the world.

International borders do not restrict foreign intelligence collection operations. You may be the target of an intelligence operation conducted by a third country, with the host country unaware of the activity. In other instances, intelligence operations directed against you may be joint efforts, with a

third country's witting support. Collection operations may be conducted by the intelligence services of foreign governments, nonintelligence-associated government ministries, agencies and research institutes, government-sponsored industry, and nonstate actors, such as private companies and terrorist organizations. Although the classic situation of a professional intelligence officer posing as a scientist to blend in at a symposium still takes place, times have changed. It is more likely that the intelligence collector sitting next to you at a symposium is someone associated with your field of expertise. Your adversary will have solid professional credentials, and he or she will be able to ask the right questions and make correct observations.

The type of information sought by foreign collectors runs the full gamut of US political, economic, industrial, and military interests. Although you may not personally possess a specific piece of technical information, you may possess operational, organizational, or personnel data that can be used by foreign intelligence collectors to identify and pursue more lucrative targets. You can reduce the possibility of becoming a target of foreign intelligence collection by taking the prudent risk-reduction steps identified in this pamphlet and by understanding the basic methods of operation employed by intelligence collectors. As an added benefit, the security measures addressed in this pamphlet are effective in reducing your risk of becoming a victim of criminal or terrorist activity or civil unrest.

Methods of Operation

Foreign intelligence collection efforts normally involve a complementary and/or redundant set of methods of operation. A nation's cultural heritage, political system, business practices and resources (time, manpower, and funding), and technical competency are all factors that will affect both the process of selecting which methods of operation to employ and how the selected method of operation will actually be used. Collection plans logically balance mission accomplishment with a minimal expenditure of resources and provide a high degree of security to the operation.

Computers and miniature electronic surveillance equipment have become relatively low-cost, effective tools, readily available to foreign governments and businesses around the world. Nevertheless, while we may be in the electronic age, traditional espionage tactics—such as agent recruitment, unwitting co-optees, sexual entrapment, or blackmail—are still being used. Usually, the foreign intelligence collector does not want to draw attention to tactics being employed, hoping to acquire the information surreptitiously. An intelligence activity directed against you will probably be conducted in an unobtrusive and nonthreatening fashion. However, in some cases foreign intelligence collection has involved more aggressive tactics, such as excessive questioning by border control officials, hotel room searches, and the outright theft of laptop computers. The following is a list of common intelligence collection techniques of which the traveler should be aware:

Elicitation— A ploy where seemingly normal conversation is contrived to extract information about individuals, their work, or their colleagues. Elicitation is subtle and should not be confused with direct questioning by government and industry representatives.

- Puts someone at ease to share information.
- Is difficult to recognize as an intelligence technique.
- Is easily deniable by an adversary.

Eavesdropping— Listening to other people's conversations to gather information. Eavesdropping activities can range from the strategic positioning of an unobtrusive bystander, to the use of concealed sophisticated audio and visual devices.

- Frequently employed in social settings where attendees feel secure and are more likely to talk about themselves and their work.
- Frequent venues include public and host-provided transportation, restaurants, bars, and meeting facility restrooms.
- Concealed devices are cost efficient, low risk, and can be used in conjunction with overt devices such as traffic and pedestrian-monitoring cameras.

Intrusion Operations—The physical entry into a room, security container, or piece of electronic equipment to steal or make reproductions of documents, magnetic and audio media, and/or the installation of electronic eavesdropping equipment. Although most intrusion operations are surreptitious, US travelers have reported returning to their hotel rooms to find individuals searching their belongings or conducting unnecessary maintenance activities. Other reported incidents of intrusion include: laptop computers showing signs of unauthorized usage or actual damage, packages having been opened and resealed or left open, locks on briefcases and suitcases missing or showing signs of forced entry, and the actual theft of the aforementioned items.

- Conducted by the host government, a foreign intelligence service of another country, or foreign business operatives.

- Frequently accomplished with the cooperation of the hotel staff.

- Several countries, and possibly foreign companies, have the ability to overcome commercial computer intrusion-protection software and hardware.

- When reported, can be explained away as a criminal activity, for example, someone looking for passports, cash, and other valuables.

Electronic Interception—The legal or illegal intercept of electronic communications. Increasingly conducted against modern telecommunications systems and personal electronic devices, such as personal digital assistants (PDA).

- Foreign telecommunications carriers are particularly vulnerable because most are government controlled.
- Office, hotel, and portable telephones are key targets.
- Facsimile, telex, and e-mail can be electronically monitored.
- Many countries have the ability to intercept and possibly break commercially available encryptions.

How To Protect Yourself

Common sense, basic security measures, and threat awareness can effectively protect you against foreign intelligence attempts to collect classified, sensitive, and proprietary information.

Some security tips you should employ include:

- Prior to departure, become informed about the foreign locations you will be visiting: the foreign intelligence collection threat; crime problems; and facilities available to you for the transport, storage, and discussion of classified, sensitive, and proprietary information. Recommended pre-travel information resources are provided on page 10.

- Provide travel arrangers and hotel staffs with only the information necessary to conduct your transactions.

- Unless specifically required, do not divulge information that identifies you as an official government or corporate traveler.

- When traveling, do not divulge information to anyone not authorized to hear such information, including specific facts pertaining to the US Government, your company, your work, and personal information about yourself or colleagues.

  - Ignore or deflect unwarranted inquiries or intrusive conversation. Provide nondescript answers.

- When in transit or when separated from your computer or PDA, utilize removable storage

mediums for sensitive and proprietary information (for example, removable floppy disks, CD-ROMs, and hard drives). Carry such items with you, separate from your computer.

- Do not discuss classified, sensitive, or proprietary information on public transport, in hotel rooms, or other public venues. Discuss US sensitive and classified information in official US facili ties cleared for discussions at the appropriate level. Business travelers should adhere to their company's security guidelines for the discussion of corporate sensitive and proprietary information.

- Do not leave classified documents or equipment unattended in hotel rooms or hotel safes; utilize appropriate US Government-authorized secure facilities.

- Do not use foreign computers, facsimile, or telephones to transmit or discuss classified or sensitive information.

- When in doubt, seek assistance from the appropriate local security representative of the US Government or your company. Report suspicious incidents.

Maintaining a Low Profile

Your behavior while overseas could increase your visibility and susceptibility to the compromise or loss of classified, sensitive, or proprietary information. In some cases, it will be hard to maintain a low profile while traveling. For example, the nature of your visit, such as attending a technical conference, will associate you with a government program or corporate project. Even the clothes you wear may draw unwanted attention. Unless required to do so, refrain from wearing US organizational or corporate logo clothes in public. This prudent step will also reduce your chance of becoming a victim of criminal activity, civil unrest, or terrorism.

Aside from being a potential intelligence target for the information you possess, scrutiny in a foreign country may occur by design or chance for some of the following reasons:

- Using commercial or government encryption programs for e-mails.
- Fitting a terrorist, drug trafficker, criminal, or other security-risk profile.
- Being involved in black-market activity such as the unauthorized purchase, sale, or transfer of tax-free US commodities.
- Having the host government discover materials on your person or in your luggage that are banned or strictly controlled.
- Associating with individuals that the government labels as dissidents.

Pre-Travel Threat Information

Before making final plans for your foreign travel, you should contact your organization's security office to ensure compliance with the foreign travel procedures of your organization and to obtain current foreign intelligence threat information.

Various US Government agencies provide security educational materials and can provide counterintelligence (CI) and security briefings for foreign travel. Your security office can obtain these materials and arrange for pre-travel security briefings. In addition, you can find up-to-date foreign travel security information on the Internet. At the very least, you can contact the Federal Bureau of Investigation Awareness of National Security Issues and Response (ANSIR) program representative for your area.

The National Counterintelligence Executive
The National Counterintelligence Executive (NCIX) was established in December 2000 by Presidential Decision Directive-75 (PDD-75), entitled "U.S. Counterintelligence Effectiveness—Counterintelligence for the 21st Century." The PDD created the NCIX to serve as the substantive leader of national-level CI and to coordinate and support the critical CI missions of the US Government. The NCIX was legislated into existence by Public Law 107-306 on November 27, 2002. The new legislation provides direction for the NCIX to initiate CI programs based on a two-way dialogue between national policy makers and the private sector. This dialogue contributes to the development of our national strategy through the understanding of what defines specific critical information, technologies, and industries, the loss of which would seriously damage the strength of our nation. The outreach activities of the NCIX, to include threat awareness

and security education publications such as this pamphlet, represent the NCIX commitment to meet the needs of government and the private sector through this two-way dialogue. Visit the NCIX web site at www.ncix.gov.

Federal Bureau of Investigation
The public voice of the Federal Bureau of Investigation (FBI) for countering espionage, terrorism, and all national security issues is the Awareness of National Security Issues and Response (ANSIR) program. ANSIR is designed to provide unclassified national security threat and warning information—specifically related to foreign-sponsored or foreign-coordinated intelligence—to US corporate security directors and executives, law enforcement, and other government agencies. Each of the FBI's field offices has an ANSIR coordinator. Additional information concerning the ANSIR program can be obtained from the FBI Web site: www.fbi.gov/ansir.

US Department of Defense
Department of Defense activities and cleared defense contractors can obtain current foreign intelligence threat information from their supporting CI activity (the Air Force Office of Special Investigations, the Army Intelligence and Security Command, the Naval Criminal Investigative Service, and the Defense Security Service).

Department of State
The Department of State established the Overseas Security Advisory Council (OSAC) to foster the exchange of security-related information between the US Government and the US private sector operating abroad. OSAC maintains a Web site that provides timely news and travel warnings at: www.ds-osac.org.

Reporting Incidents

The first line of defense against foreign intelligence collection operations is in your hands: the reporting of suspicious incidents. US Government and cleared defense contractor employees are required by regulation to report such incidents. The US business community, while not required by law to make reports, should recognize that cooperating with the Federal Government is in the best interest of all parties. In addition, your company may have specific employee regulations that require the reporting of suspicious incidents. Remember, there are federal agencies specifically tasked to receive, analyze, and act upon suspicious information. The reports you make are used to identify the "who, what, why, when, and where" of foreign intelligence collection.

Do not hesitate to report even seemingly minor incidents. As mentioned in the section on methods of operation, foreign intelligence operations normally employ a complementary and/or redundant set of methods of operation. What appears to be an isolated incident, will many times be part of a larger collection operation. For example, CI specialists were able to link an overseas targeting incident to what appeared several years before to be an innocent foreign request to conduct postgraduate training with a US company. Report all suspicious incidents.

Referral of Suspicious Incidents While Overseas

Before your departure from the United States, you should review the procedures of your organization

for reporting suspicious incidents. When overseas, suspicious incidents should be reported to the nearest US diplomatic facility. When reporting incidents to overseas corporate security representatives, ensure that only properly cleared US persons are involved in discussions of US sensitive, classified, and export-controlled information. You should also report the incident to your organization's appropriate CI and/or security component as soon as possible upon your return to the United States.

Referral of Suspicious Incidents in the United States

Suspicious incidents should be reported in accordance with the procedures of your organization. In general, the following US Government agencies should be contacted:

- **Federal Bureau of Investigation**
  Suspicious incidents should be reported by the private sector to the local FBI Field Office. Consult your local phone directory for the telephone number. Employees of the US Government and cleared defense contractors will report suspicious incidents to the FBI and to the CI activity supporting your organization, in accordance with established procedures. Your Security Officer can provide reporting procedures, as well as information regarding applicable Federal laws, regulations, and contractual requirements.

- **US Department of Defense**
  Department of Defense military and civilian employees will report all suspicious incidents to the supporting Military Department CI activity in accordance with the procedures established by your organization. Your Security Officer can provide information on the CI activity point of contact for reporting suspicious incidents.

  Employees of cleared defense contractors will report all suspicious incidents to their Facility Security Officer (FSO). Your FSO will forward the information in accordance with the National Industrial Security Program Operating Manual (DoD 5220.22-M) to the Defense Security Service or to the CI activity of the designated Cognizant Security Authority.